Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

~ Landfill Games Sell! ~ People Are Talking! ~ Google Gets Fined!
~ Search for Every Tweet ~ Call of Duty: Heroes! ~ Sexism Game Ratings?
~ Atari Chips Available! ~ Google, Rockstar Suit! ~ Detect Gov't Spyware!

~ AT&T Kills Permacookie ~ "Far Cry" New Heights! ~ Yahoo Over Google!

-* NSA Warns of China Attacks! *-
-* State Dept. Network Breach Shutdown *-
-* New U.S. Web Rules Must Withstand Lawsuits *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

There's so much to talk about this week! Record snowfall in the Buffalo area - have you seen the pictures?!? How about the arrogance of our president taking "executive action" and making a major decision regarding immigration - 5 million undocumented immigrants to basically get amnesty!? You know what, I'm not going to focus in on those news items this week. regardless of the significance.

What I am going to quickly focus on this week is next week's holiday, Thanksgiving. As I've been saying for many, many years now, this is one of my favorite holidays. It's a time to be with family, and enjoy a wonderful feast. As usual, we typically have a small celebration at home - my wife and I, and our 4-legged "children". This year, we'll be missing one of those "children" - we had to put one of them down earlier this week. But, she'll be with us in spirit - that's how much of an impact she had in our lives.

So, one suggestion I can put out there this year - enjoy these types of holiday celebrations to their fullest, with family and friends. Because, if you think about it, you may not have the same opportunity next year.

Happy Thanksgiving!

Until next time...

=~=~=~=

New Atari Chips Available

Hello,

I will enter a small quantity of MC68060RC50 rev.6 (71E41J) mask able to run at 95-100 MHz.

Maybe more with RC60 : I never get and tested RC60 with this mask...so maybe we will have a good surprise (running higher freq).

The rev.6 060 are now very rare and difficult to find (sure there are many 10.000 is stock of big distributors but à 400-500$!!).

And there are many fake on the market (re-printed dummy mask on the CPU !)

My price is 120 + shipping = 5 for Europe and 10 for rest of world.

If you want one, please send money now on my paypal account (my email).
Please counterbalance the pp fees that I will not get (around 3%).
This give you a PP price of 124 .

You can pay by Western Union or cash by secured postal letter.
Just inform me.

Regards
--
Rodolphe Czuba

http://rodolphe.czuba.free.fr/
www.powerphenix.com
www.yonnesolaire.fr
4, che du guØ des Archers
Fontaines
89150 St ValØrien
FRANCE

=~=~=~=

->In This Week's Gaming Section - Call of Duty: Heroes!
  """""""""""""""""""""""""""""""   'Far Cry' Aims for New Height!
                                     Sexism Ratings for Games
                                     And much more!

=~=~=~=

->A-ONE's Game Console Industry News   - The Latest Gaming News!
  """""""""""""""""""""""""""""""""""""

Call of Duty: Heroes Is Clash of Clans with Guns

If the blockbuster action and Kevin Spacey-ness of Call of Duty: Advanced Warfare isn't enough to scratch your militaristic itch, there's now yet another way to take your Call of Duty addiction on the go. Taking some major design cues from hit mobile strategy game Clash of Clans, Call of Duty: Heroes has you attack and defend military bases using characters and weapons from Activision's popular first-person shooter franchise. The free-to-play game is available now in iOS and Windows devices, with an Android version on the way.

As with Clash of Clans, Call of Duty: Heroes' core gameplay cycle consists of using resources to fortify your base, training fighters for battle and attacking enemy strongholds. Whether you're invading a base or

defending your own, combat is as simple as tapping the screen to deploy your soldiers and watching the action unfold. The game lets you take on other players in PVP mode as well as defending against increasingly-difficult waves of enemies in survival mode.

Heroes sets itself apart with some action-oriented mechanics lifted from the Call of Duty console games, such as the ability to rain down fire from above with a helicopter turret. The game’s Heroes - leader characters with special abilities - are also lifted from the core series, with the option to take control of characters like Captain Price from Modern Warfare and Mike Harper from Black Ops 2.

Heroes is far from the first Call of Duty mobile game; previous installments like Call of Duty: Strike Team and Call of Duty: Black Ops Zombies emulate the first-person shooting gameplay of their console counterparts, whereas Activision’s new Heroes game aims to capitalize on the ever-growing mobile strategy genre.

I had a good time deploying troops and ordering chopper strikes during my brief time with Heroes, and the game seems like a perfect fit for those who don’t mind a Call of Duty skin over Clash of Clans’ signature gameplay. As with most free-to-play games, you’ll likely have to either spend real money or lots of time in order to build the ultimate base, but the title is enjoyable enough in small bursts.

’Far Cry’ Video Game Aims for New Height - The Himalayas

Ubisoft is out to build on the success of its "Far Cry" video game franchise with a new installment promising players more choices and smarter enemies in an expansive world.

The action-adventure game set for release on Tuesday will be the fourth edition in the series, which has sold a reported 20 million copies since the first version was released in early 2004.

About half of those sales have been credited to "Far Cry 3," which won legions of fans after it hit the market at the end of 2012.

"Far Cry is a sleeper in some ways, but it is building momentum," analyst Scott Steinberg of high-tech consulting firm TechSavvy told AFP.

"It has become a popular franchise but still has plenty of room to grow."

"Far Cry 4" due out on Tuesday was billed as the most expansive and immersive version yet of the open-world, first-person shooter game.

While its predecessor played out on a tropical island, the story in "Far Cry 4" is set in a fictional region of the Himalayas serving as a stronghold for a self-appointed despot.

"The first idea for Far Cry was not to put it in the mountains; it was that someone on the team wanted to ride an elephant," game executive director Dan Hay told AFP while providing an early glimpse at the new version.

"Maybe we took a hard road, but we asked what we wanted to do as game players."

The Montreal Ubisoft studio behind the game set out to imbue "Far Cry 4" with features people loved in its predecessor and unexpected new twists.

For example, players can indeed ride elephants while attacking mountain fortresses that Hay described as "outposts on crack that can fight back."

Artificial intelligence built into the game has resulted in virtual enemies even surprising its creators with reactions to situations.

Even the fictional villain in the game, a character named Pagan Min, is billed as deviously insightful.

"Everyone has that friend in the past who was bad for them," Hay said while describing Pagan Min.

"They are a blast to hang out with; but if you hang out with them you are going to wind up dead or in jail. This is that guy."

Along the way, the new version of Far Cry calls on players to choose between tradition and seizing new opportunities in the Himalayan realm.

"Far Cry asks you to take a digital year of your life and meet credible characters who will challenge your assumptions," Hay promised.

"After finishing school we start with the idea that we are going to get it right; better than our friends or parents - Far Cry gives you the choice."

Versions of the game for play on current and previous generation Xbox or PlayStation consoles, as well as on computers powered by Windows software, will launch at a price of $60, according to France-based Ubisoft.

Spectacular Dragon Age: Inquisition Burns Bright

The most useful item I used while playing Dragon Age: Inquisition? A bottle of eyedrops.

I probably should have used a few bottles, actually, because I don t think I blinked more than a handful of times during the dozens of hours I spent saving the land of Thedas from demonic hordes in the latest role-playing masterpiece from genre kingpin Bioware. Marrying the best bits from the first two Dragon Age games, it s a must-have for gamers with plenty of time on their hands.?

It s a daunting proposition for those new to the franchise, though. Inquisition is the third Dragon Age game, and while Bioware wisely tossed together a handy website that lets you quickly whip through the biggest decision points in the first two games to set up a World State for the new one, you re probably best off playing through at least one prior Dragon Age before diving in.

It s not required, however, as Inquisition features a standalone story and casts you in the role of a brand-new character. You re the Herald of Andraste, the unlikely survivor of a calamitous explosion that tore a hole in the sky and killed off a collection of world leaders. That hole was just one of many, and through these breaches pours a steady stream

of toothy unpleasantness. So off you go, gallivanting across the land as a member of the fact-finding, world-saving Inquisition in an effort to heal old wounds, unite warring factions, plug up the sky holes, and find out who or what is behind the apocalyptic mess.

It s classic Dungeons and Dragons-esque stuff, letting players build a dwarf, elf, human, or bull-like Qunari hero using a shockingly powerful character creator. But where plenty of fantasy games let you cast spells and swing swords, Dragon Age: Inquisition lets you do these things on a scale not seen since the incredible The Elder Scrolls V: Skyrim.

It s not an open world, however; each of the game s many explorable regions is zoned off from the rest, though they re all expansive and filled with enough sidequests, lore, and random encounters to easily blow up a few weekends. The frustrating linearity of Dragon Age II s smallish areas have been ditched in favor of big, unique playgrounds in which to roam freely. The developers even saw fit to add a jump button, encouraging you to leap off a ledge and scour the wilderness for goodies. It s a bit too clean compared to the glorious messiness of Skyrim, but it s easily the best world-building we ve seen yet in Dragon Age.

You ll spend the bulk of your time in the trenches, running missions, working through conversation trees, wooing possible mates, and fighting, fighting, fighting. The combat blends the fussy, pause-the-action strategy of the first game with the button-mashy action of the sequel, and it hums along nicely. Swapping between your four active party members (pulled from a much larger stable) is quick and easy, though most of the time you can just focus on your character and let the A.I. handle your companions.

While you don t need to micromanage this stuff, you certainly can (and likely will). I torched hours tweaking the gear, abilities, and even artificial intelligence of my party. Learning the ins and outs of each mage, warrior, and rogue is super helpful when you get into the bigger, nastier fights. That dragon isn t going to just let you whack it on the foot for an hour, you know.

There s plenty to manage in Dragon Age: Inquisition. A war table lets you marshal spies, diplomats, and armies around Thedas to gather resources and open up new areas to explore. As the Inquisition s influence spreads, you ll gain permanent boosts and new dialogue options. Every ounce of energy you put into this game gives you something in return, and while it s a little intimidating at first, soon enough you ll find yourself joyfully flopping around in its myriad game systems like a kid in a ball pit.

Veering off the main story is so easy, in fact, that it speaks to Bioware s trouble keeping the plot focused and sharp. While the game s huge cast of characters shines, Thedas complicated sociopolitical landscape occasionally drags the narrative into the weeds. Some of the game s brightest moments and most essential missions lie off the beaten path.

Dragon Age: Inquisition s sheer size also proves problematic, though I experienced relatively few glitches playing the Xbox One version of the game (PS4 players have reportedly had a rougher go). An interface stallout here or there required me to backtrack to an earlier save. The old Save early, save often refrain definitely applies here.

While it occasionally hiccups, Dragon Age: Inquisition is, at times, flat-out gorgeous. The creature design is terrific, recalling enemies from past games but dialing up the look and feel. The first time you encounter a dragon in this case, a big, irritated one flying around, coughing up fireballs you ll marvel at its fluid movements and intimidating presence. Then you ll die, because it s a dragon, and you re probably not ready for that yet.

You re also probably not ready to dive into the game s multiplayer. Separated entirely from the solo campaign, it s a story-free cooperative dungeon-crawling sort of affair in which you kill enemies and gain loot and gold. It s not bad, but it s not enticing either. It s a wisp of weird icing on a 15-layer cake.

Besides, you ve got a land to save, a rogue to flirt with, a hole to fix, and a dragon to slay. Big, meaty, and unequivocally fun, Dragon Age: Inquisition improves upon the first two games in just about every way. Grab some Visine and give it a stab.

Swedish Trade Group Proposes Sexism Ratings for Games

Sweden-based industry trade group Dataspelsbranchen is researching a new content rating system for video games based on promotion of gender equality.

The proposed ratings system, inspired by the Bechdel test, will examine how in-game female characters are portrayed with regard to equality and diversity. The group recently received a 272,000 kronor (nearly $37,000) grant from Sweden’s government-funded Vinnova agency to further its research.

"I do not know of any other project in the world asking this question and of course we want Sweden to be a beacon in this area," project manager Anton Albiin told Swedish publication The Local. "Of course games can be about fantasy but they can be so much more than this. They can also be a form of cultural expression - reflecting society or the society we are hoping for. Games can help us to create more diverse workplaces and can even change the way we think about things."

The group’s research follows up on recent concerns raised by Anita Sarkeesian and other media critics, who highlight the one-dimensional treatment women characters often receive in video games.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!

Atari Games Buried in Landfill Net $37,000 on eBay

What some have called the worst video game ever made has fetched thousands of dollars for a New Mexico city.

An old "E.T. The Extra-Terrestrial" game cartridge drew the highest bid among 100 Atari games auctioned on eBay by Alamogordo officials.

The games were part of a cache of some 800 Atari video games buried more than 30 years ago in a landfill and dug up in April.

Joe Lewandowski, a consultant for the film companies that documented the dig, says the online auction, which ended Thursday, generated $37,000.

"It’s really gratifying to see that happening because again to everybody it was a bunch of garbage in the landfill. You’re kind of nutty to go dig it up," Lewandowski told KRQE-TV.

The "E.T." game, still in its original box, sold for $1,537 to a buyer in Canada. The interest in the games has gone global. According to Lewandowski, online bidders from other countries including Germany and Sweden snapped up items. Earlier this month, a museum in Rome opened an exhibit on the dig that includes dirt from the landfill.

"I keep getting messages from people around the world asking me if there’s any more left, it’s crazy," Lewandowski told the Alamogordo Daily News. "The people that lost the bids are demanding more but I keep telling them they have to keep checking."

Reports that truckloads of the game were buried in the landfill have been urban legend since the early ’80s. The "E.T." game’s poor reception when it came out in 1982 was seen as a factor in Atari’s demise.

City documents show that Atari consoles and more than 1,300 games were found, including "E.T. the Extra-Terrestrial." Some of the other discovered titles include "Centipedes," ’’Warlords" and "Asteroids."

After months of planning with state and local regulators, crews discovered numerous game cartridges on April 26. The dig cost more than $50,000, Lewandowski said.

LightBox Entertainment and Fuel Entertainment pursued the dig for a documentary that is due to come out Thursday.

Alamogordo owns the cartridges because they came from the city’s landfill. The revenue will go to the city and the Tularosa Basin Historical Society. Both groups will meet Dec. 1 to discuss how to spend the money.

The remaining game cartridges will be sold on eBay over the next few weeks.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

US State Department Network Shut After Cyber Breach

The US State Department said Monday it shut down its unclassified computer network over the weekend after evidence emerged that it could have been hacked.

Officials believe the incident "was linked" to one late last month when hackers breached the White House’s unclassified computer network, State Department press office director Jeff Rathke told reporters.

The State Department had initially said in an email late Friday that the shutdown came as scheduled routine maintenance to its main unclassified network, and would impact email traffic and access to public websites.

But on Monday, Rathke said the department had recently detected "activity of concern" in portions of the system handling non-classified emails, and the weekend maintenance included security improvements responding to the breach.

"We have no reason to believe classified information was compromised," Rathke told reporters.

He said the State Department’s secure, internal communication system within the building and linking US diplomatic posts worldwide were operational, but that the Internet-connected systems remained down on Monday.

"We are implementing carefully planned improvements to the security of our main unclassified network, taking advantage of a scheduled outage," Rathke added. "No classified systems have been affected by this incident."

Rathke said the origin of the cyber breach and who might be responsible is "something that remains under investigation."

The State Department is the latest in a series of government agencies to face cyber security breaches.

Last month, the White House reported an intrusion in its unclassified computer network.

In the course of addressing the breach, some White House users were temporarily disconnected from the network but the computers and systems were not damaged, an official said.

The Washington Post quoted sources as saying hackers believed to be working for the Russian government were believed to be responsible for that breach.

Last week, the US Postal Service said hackers stole sensitive personal information from its employees in a large data breach this year, and got took some customer data as well.

A USPS spokesman said the breach affected as many as 800,000 people who are paid by the agency, including employees and private contractors.

NSA Chief Warns Chinese Cyber Attacks Could Shut U.S. Infrastructure

China and "probably one or two" other countries have the ability to invade and possibly shut down computer systems of U.S. power utilities, aviation networks and financial companies, Admiral Mike Rogers, the director of the U.S. National Security Agency, said on Thursday.

Testifying to the House of Representatives Intelligence Committee on cyber threats, Rogers said digital attackers have been able to penetrate such systems and perform "reconnaissance" missions to determine how the networks are put together.

"What concerns us is that access, that capability can be used by nation-states, groups or individuals to take down that capability," he said.

Rogers said China was one of the countries with that capability, but that there were others.

"There's probably one or two others," he said, declining to elaborate in a public setting.

Rogers testified two days after a bill to overhaul the NSA's bulk collection of telephone records failed in the Senate. Privacy advocates will probably now have to start over to pass a law to reform U.S. surveillance rules.

He said at the hearing that telephone companies are still providing those records to the NSA, but under stricter rules than when the program was exposed in 2013 by former contractor Edward Snowden.

Rogers said the agency, anticipating passage of a new law, would wait before moving forward with technological changes. He said the agency, and telephone companies, would rather wait and see what might be included in any new law.

AT&T Kills The 'Permacookie,' Stops Tracking Customers' Internet Usage

In recent weeks, Verizon and AT&T have been caught up in a privacy firestorm over their use of so-called "permacookies," a method of tracking what their users do while browsing the Web with the intent of sharing that data with advertisers. Verizon's permacookie program lives on, but AT&T has ceased the practice, ProPublica reported on Friday.

At least for now.

AT&T tells ProPublica that its use of permacookies was "part of a test," which has since wrapped up, but the company says that it "may still launch a program to sell data collected by its tracking number." For its part, AT&T says that it will allow customers to opt out of the program if or when it decides to use permacookies for advertising purposes.

The story behind the story: Permacookies aren't cookies in the traditional sense: Instead, they're unique identifiers appended to website addresses you type in on your device that let carriers see what

kinds of sites you visit.

Permacookies exist for the same reason traditional tracking cookies exist so advertisers can see what sorts of things you might be interested and serve up related ads in the hopes that you'll click on them. But unlike regular tracking cookies, which you can easily delete from your browser or block entirely, there's no way of removing or blocking permacookies since they're handled entirely by the carrier.

Despite the outcry from consumers and activists, it's hard to shake the feeling that permacookies aren't going away now that the proverbial cat is out of the bag. Both Verizon and AT&T have said they allow (or will allow) customers to opt out of the advertiser data sharing program, as ProPublica notes (though Verizon won't let you opt out of the identifier program), but you're still very much at the mercy of the carriers.

If you're on Verizon and are concerned about the privacy implications, our Ian Paul has a couple suggestions: First, use Wi-Fi instead of the cellular network whenever possible so you bypass Verizon's network entirely. If that's not practical, though, consider using a VPN to help keep your Web browsing private.

Any New U.S. Internet Rules Must Withstand Lawsuits: FCC Chief

U.S. regulators expect Internet service providers to sue the government over any changes in the way they are regulated and must reevaluate any proposals to make sure they stand up in court, Federal Communications Commission Chairman Tom Wheeler said at a meeting on Friday.

Last week U.S. President Barack Obama said Internet service providers should be regulated more like public utilities to make sure they grant equal access to all content providers. This touched off intense protests from cable television and telecommunications companies and Republican lawmakers.

"Let's make sure that we understand what is going on here. The big dogs are going to sue regardless of what comes out," Wheeler said.

"We need to make sure that we have sustainable rules, and that starts with making sure that we have addressed the multiplicity of issues that come along and are likely to be raised," he added.

Wheeler did not explicitly address the reclassification of Internet service providers and a spokesman said he is still evaluating multiple options. Experts have said reclassification could be challenging to argue in court. A decision is not expected before 2015.

On Nov. 12, AT&T Inc said it would stop investing in high-speed Internet connections in 100 cities until the Web rules were settled.

Google Fined For Not Taking Down "Right To Be Forgotten" Links Worldwide

A French court has convicted Google of failing to comply with a right to be forgotten case after it took down links on its French subsidiary but

failed to do so globally.

Dan Shefet, a lawyer practicing in France, first sued the subsidiary in August 2013 over defamation lodged at him and his firm by a gossip site that, among other things, falsely accused him of losing his licence to practice law in France and Denmark.

The French court sided with Shefet and told Google to yank certain URLs on a worldwide basis.

Google, however, only took down the sites from google.fr and, according to Shefet, ignored subsequent demands based on the court order.

Removing links from sites ending in ".fr" didn't help matters much, Shefet said, given that his clients include those from other countries.

Now, the French child is paying for the sins of its US parent.

A judgment handed down in September by the Paris Tribunal de Grande Instance means that Google France is facing fines of 1,000 ($1,252, £799) a day, plus 1,500 to cover the plaintiff's costs.

According to Shefet's lawyer, this decision against how Google treats takedown requests worldwide is a first not only in France but in Europe.

The French court isn't the first to order Google US to bury search results, mind you. Canada got there before it.

In June, a Canadian court ruled that Google had to bury search results for a Canadian company's competitor, not just in Canada but around the world.

A month later, the Court of Appeal of British Columbia had given the go-ahead for Google to appeal the decision, but it refused to stay enforcement of the injunction.

The French court's decision may now bolster other European courts in their efforts to impose court orders on online companies beyond their own borders.

The decision relies on the European right to be forgotten: a ruling by the European Court of Justice (ECJ) that handed victory to a Spanish man who wanted Google to remove links to an old article saying that his home was being repossessed to pay off debts.

In the French case, Google's lawyers had tried to get the removal limited to links on google.fr, but the judge, relying on the reasoning in the ECJ's ruling, rejected the attempt, saying that Google and its French subsidiary are inseparable.

From that ruling:

The activities of the operator of the search engine and those of its establishment situated in the member state concerned are inextricably linked.

Shefet predicts that the decision will give European courts a new tool in forcing Google to forget things worldwide. It's not just about privacy or defamation, he said, but rather could substantially alter the entire range of business liabilities for multi-national corporations with local subsidiaries.

The Guardian quotes him:

The real importance of those decisions is that now any individual in the UK or another member state who suffers from Google s [links to a libelous article] may obtain an injunction against their local Google subsidiary.

Until now a subsidiary could not be legally forced under the threat of daily penalties to deliver a result which was beyond its control. The complainant would therefore have to obtain judgment against Google in the US because only Google Inc controls the search engine world wide.

Now a daily penalty can be inflicted upon Google UK by local courts until Google Inc delivers the result by way of [removing links] world wide.

But while the European Union's power to drown links seems to have gotten stronger, back in Google's home country, the opposite is happening, with a San Francisco Superior Court judge last week upholding the already widespread legal opinion in the US that search results constitute free speech.

That means, the judge decided, that the owner of a website called CoastNews had no right to sue Google for putting CoastNews too far down in search results, while Bing and Yahoo were turning up CoastNews in the number one spot.

In its latest transparency report, Google said that since it launched the removal request process on 29 May 2014, it's received 169,668 takedown requests.

It's complied with a minority - 41.7% - of those requests, removing links pertaining to, for example, a German rape survivor who asked the company to remove a link to a newspaper article about the crime when people search on the individual's name.

It's refused to take down links to articles that are merely embarrassing or which are related to business as opposed to private matters, such as that from a British media professional who wanted to bury embarrassing content he posted.

According to the Guardian, Google is considering its options regarding the French decision, including a possible appeal. It says that it already removes links to defamatory online articles, thereby fulfilling its legal obligations to French citizens.

The Guardian quotes a Google spokesperson:

This was initially a defamation case and it began before the ruling on the right to be forgotten. We are reviewing the ruling and considering our options. More broadly, the right to be forgotten raises some difficult issues and so we re seeking advice both from data protection authorities and via our Advisory Council on the principles we should apply when making these difficult decisions.

Google and Rockstar Wind Down Their Year-long Patent War

The high-profile patent lawsuit between Google and the "Rockstar Consortium" is drawing to a close. Google has signed a "term sheet" with Rockstar, which will be finalized as a settlement in the coming weeks.

The lawsuit has been closely watched, especially because Rockstar is owned by some of Google's chief rivals in the smartphone industry: Apple, Microsoft, Blackberry, Ericsson, and Sony. The Rockstar group was created in 2011, and it bid $4.5 billion for the large patent portfolio of Canada-based Nortel, which went bankrupt in 2009.

None of the terms of the Google-Rockstar settlement have been made public so far. The news comes days after it became public that Cisco expects to take a $188 million charge to settle its own patent dispute with Rockstar, which sought royalties from at least a dozen Cisco customers.

Rockstar's lawsuit against Google was filed in October 2013. Motions filed in the Texas case indicate it was moving through the discovery process, even though earlier there had been a great deal of fighting over venue.

A court document (PDF) filed Monday revealed that Google and Rockstar had settled, "in principle, all matters in controversy between the parties," and the two sides signed a term sheet. It isn't clear if the deal will also resolve Rockstar's allegations of infringement against Google's Android partners who got sued, including Samsung and HTC.

A Google spokesman declined to comment.

Free Tool Detects Government Spyware

Governments all around the world use malware and spyware to keep tabs on people, from visitors to residents. But a security researcher's tool can now determine if your computer is infected with spyware.

The Detekt tool was developed by Berlin-based security researcher Claudio Guarnieri and supported by several human-rights groups. Detekt is checks for malware that is often used against journalists, activists and other people frequently targeted by governments.

Available as a free download, Detekt is primarily a scanner; its primary purpose is to warn users if they're being spied on, not to remove that spyware. If Detekt does detect spyware, the researchers recommend users disconnect that computer from the Internet and stop using it immediately. Then, users should contact an expert via a computer they don't normally use.

Lists of experts who may be able to help, along with their PGP keys for sending encrypted emails, are available from Detekt's website.

Detekt is currently compatible with Windows XP, Vista, 7, 8 and 8.1. It's available in English, German, Italian, Spanish, Arabic and Amharic, the national language of Ethiopia.

According to Amnesty International, one of Detekt's co-sponsors, an early version of the tool was used to investigate surveillance practices in several countries. Detekt discovered that several human-rights lawyers and activists in Bahrain were being spied on with a commercial piece of spyware called FinSpy.

Amnesty International warns that Detekt can’t magically detect all spyware; rather, it is designed to recognize some of the most commonly used and encountered commercial spyware. The developers will continue to update Detekt as the spyware it targets evolves and changes.

"The growing trend in indiscriminate mass surveillance on a global scale was laid bare by the Edward Snowden disclosures," writes Amnesty International in its post on Detekt. "Following the lead of the USA and other industrialized countries, governments everywhere now justify the use of such surveillance. This has a chilling effect on the rights to freedom of expression and peaceful assembly in countries across the world."

Twitter Update Now Lets Users Search Every Public Tweet Ever Sent

It’s now surprisingly easy to search your own embarrassing Twitter history - or that of any user.

Twitter updated its search tool today to allow users to search through the ever-growing list of a half trillion tweets that have been sent over the past eight years.

"Our long-standing goal has been to let people search through every Tweet ever published," Yi Zhuang, a search infrastructure engineer at Twitter, said in a blog post.

The search functionality remains the same, however, users will notice that Twitter now displays all relevant results. Previously, more current tweets with the highest engagement dominated the results.

Zhuang said the improved search infrastructure is ideal for getting the entire conversation, whether it’s for a sports season, a conference or a trending hashtag, such as #Ferguson.

Twitter gave users the option in 2012 to download their personal library of tweets, however the new search capability is also ideal for quickly finding anything from your tenure on Twitter.

Simply type in a person’s username plus a keyword and marvel at how easy it is to dig up the past.

Google Launches Service To Remove Ads from Websites

Sick and tired of all those ads? Google is testing a program called Contributor that lets you subscribe to the Web.

Well, not to the whole Web just to 10 Web publishers that are participating in the Contributor experiment. Under it, people pay $1 to $3 per month and see a thank-you note on websites instead of an advertisement.

When you visit a participating website, part of your contribution goes to the creators of that site, the Google Contributor site said. The

more you contribute, the more you support the websites you visit.

The thank-you note appears in place of an ad that Google otherwise would have supplied, spokeswoman Andrea Faville said. The 10 publishers participating in the experiment include photo-sharing site Imgur, news satire site The Onion, tech news site Mashable and slang-explanation site Urban Dictionary.

Google Contributor is an interesting idea for a company that s funded by ad revenue, but so far, it is only an experiment. Google offered a waiting-list form to let people sign up.

Free, ad-supported content has proved a popular way to quickly launch Internet-based services, and advertising is the financial lifeblood behind services such as Facebook s social networking, Twitter s information feed, and Google s search.

But in some eyes, advertising has a dark side, too: Ads work better if they re targeted at people who are likely to find them interesting, and that means those who operate websites have an incentive to track personal information. The common expression of this complaint is that people s personal data becomes the product website operators sell to advertisers.

Google indicated that a Google Contributor subscription would, in effect, mean that a person was paying for privacy as well as an ad-free experience.

Use of this service will not be used to target ads, Faville said.

Advertisers are expected to spend $141 billion on online ads this year, and that number should increase annually more than 15 percent in 2016, according to eMarketer. Google is the top beneficiary by far this year, receiving an estimated 32.4 percent of that total. Facebook is next at 8 percent, followed by Microsoft at 2.9 percent and Yahoo at 2.4 percent.

In the news media, sites like The Wall Street Journal, The New York Times and The Financial Times keep some of their content behind subscription paywalls, but that can significantly reduce readership compared to free, advertising-supported content. Some critics, however, believe that ad-driven news sites have too strong a financial incentive for producing sensational articles that will mean lots of page views.

It s also not clear exactly how Google will split the subscription revenue with the publishers though that s no change from the existing situation showing Google ads. The amount we keep is the same we charge advertisers to show their ads, Faville said.

The more a person pays, the more he ll see ad-free sites, and websites shouldn t see a difference in revenue, Google said. In terms of the rates, the amount that goes to the publishers is essentially the market rate for ad space on their site (in the ad auction). So the amounts going to publishers wouldn t really be affected, although the higher the amount in a person s Contributor account, the more times they would see the thank-you messages versus ads, Faville said.

The vast majority of Google s revenue comes from advertising. In the third quarter, Google raked in $16.52 billion. Of that, Google returned $3.35 billion to sites that carried its ads or that referred search traffic that led to search ads.

Some of that revenue comes from search ads that show up next to search results, but it also shows more graphic display ads on sites that choose to use its DoubleClick service. DoubleClick is used for direct and indirect advertising. For example, you may see a DoubleClick-supplied ad on a Google property like YouTube, a privilege for which an advertiser, of course, pays. But you can also see a DoubleClick-supplied ad on a news site, in which case the advertiser s payment is split between Google and the news site publisher.

Yahoo Replaces Google as Firefox’s Default Search

Yahoo will supplant Google’s search engine on Firefox’s Web browser in the U.S., signaling Yahoo’s resolve to regain some of the ground that it has lost in the most lucrative part of the Internet’s ad market.

The five-year alliance announced Wednesday will end a decade-old partnership in the U.S. between Google Inc. and the Mozilla Foundation, which oversees the Firefox browser. The tensions between Google and Mozilla had been rising since Google’s introduction of the Chrome browser in 2008 began to undercut Firefox. Google’s current contract with Mozilla expires at the end of this month, opening an opportunity for Yahoo to pounce.

Even though Chrome is now more widely used, Firefox still has a loyal audience that makes more than 100 billion worldwide search requests annually.

Yahoo is hoping to impress Firefox users as the Sunnyvale, California, company sets out to prove that it’s still adept at Internet search after leaning on Microsoft’s technology for most of the results on Yahoo’s own website for the past four years.

Financial details of Yahoo’s Firefox contract weren’t disclosed. In a blog post, Mozilla CEO Chris Beard said the new deal offers "strong, improved economic terms" while allowing Mozilla "to innovate and advance our mission in ways that best serve our users and the Web."

Google accounted for 90 percent, or about $274 million, of Mozilla’s royalty revenue in 2012. Mozilla hasn’t released its annual report for last year.

Besides dropping Google in the U.S., Mozilla is also shifting Firefox to Baidu’s search engine in China and Yandex in Russia. Firefox users still have the option to pull down a tab to pick Google and other search engines as their preferred way for looking up information online.

Yahoo Inc. CEO Marissa Mayer, a former Google executive, hailed the Firefox agreement as Yahoo’s most significant partnership since forging the Microsoft deal in 2009.

"We believe deeply in search it’s an area of investment and opportunity for us," Mayer wrote in a Wednesday blog post.

Yahoo plans to unveil a "clean and modern" search engine on Firefox next month and then roll out the new model on its own website early next year, Mayer wrote.

The redesign will primarily affect how Yahoo’s search engine’s results are displayed, and not the way that requests are processed. The search technology will continue to be provided by Microsoft Corp. as part of a 10-year deal Yahoo signed in 2009, according to Mel Guymon, Yahoo’s vice president of search.

In various public remarks since becoming Yahoo’s CEO two years ago, Mayer has expressed disappointment with Microsoft’s search technology. That has spurred speculation that she might renegotiate or end the Microsoft search partnership next year when Yahoo has an option to re-evaluate the deal. Yahoo currently receives $88 of every $100 in revenue generated from ads posted alongside the search results on its website.

Those payouts have helped Yahoo boost its revenue from search advertising for 11 consecutive quarters, compared with the previous year. Despite those gains, more searches have been shifting to Microsoft’s Bing search engine, causing Yahoo to slip further behind its rivals. Yahoo is expected to end this year with a 5.6 percent share of U.S. search advertising revenue, down from 6.6 percent in 2012, according to the research firm eMarketer.

Yahoo’s stock gained 52 cents to $51.10 in extended trading Wednesday. The shares have been hovering around their highest levels in more than 14 years, largely because Yahoo owns a large stake in Alibaba Group Holding Ltd., a rapidly growing e-commerce site in China.

Jolla Unveils Tablet, Funded in Less Than Three Hours

During an emotional speech delivered today at the Slush conference, Jolla’s Marc Dillon unveiled the company’s next product: the Jolla tablet, running Sailfish OS 2.0. He launched a crowdfunding campaign for the tablet, with a goal of $380,000 - which was achieved in less than three hours (this may be one of the fastest funding consumer electronics devices ever). I got in early, and was one of the very first people to back the tablet (just as I was one of the first to back the Jolla phone a year ago). A second round has already been announced. Big news for American readers: it’ll be available in the US too.

The tablet itself is very similar in specifications to Nokia’s N1 tablet, with an 1.8GHz quad-core Intel processor, 2GB RAM, 2048x1536 330ppi 7.85" IPS display, 32GB storage, and all the usual sensors and ports you have come to expect. It’s quite light and compact, and has its own design - there’s no way people are going to twist this one into an iPad copy.

The tablet is expected to be delivered to us early backers in May 2015, and I can’t wait. Also, Mr. Dillon, keep rocking that beard.

10 Top Security Threats of 2014 (So Far)

The top security threats of 2014 include equal parts old mistakes, new adversaries, innocent human nature and the evil that men - and women, and others - do.

In 2013, Snowden changed a conversation (and created careers for believers

across a spectrum of dark and light). Some, but not all, survived security nightmares credited to Blackhole, the SEA, and Cryptolocker. We said goodbye to Silk Road, and popular consciousness said hello to the mega retail breach with Target.

In contrast, 2014 turned the dial to 11 for infosec disasters and threats - and the egos all around them.

It was the year of super mega retail breaches, China coming to the fore in attacks, Facebook scams getting out of hand, Shellshock and Heartbleed (who brought a pet POODLE), and application security became the weakest link through a combination of its own faults and the time-honored practice of the irresponsible the blame game.

Let’s countdown the top security threats of 2014...

10. Normal people

One email spiked with innocuous-looking malware to a vendor cost Target an estimated 40 million credit cards and 70 million user accounts at the crest of 2014, beginning a year which made our own employees, coworkers, friends and family one of the biggest security threats of the year.

Target’s December disaster came from a phishing attack sent to employees at an HVAC firm it did business with. Phishing is an incredibly popular attack - because it works. Non-technical people were 2014’s favorite targets for malicious hackers, from data dealing crime rings to targeted corporate espionage attacks.

IT Security in the Snowden Era

The Edward Snowden revelations have rocked governments, global businesses, and the technology world. Here is our perspective on the still-unfolding implications along with IT security and risk management best practices that technology leaders can put to good use.

F-Secure’s Mobile Threat Report Q1 2014 was a bucket of cold water in terms of just how pervasive attacks on typical users are, and how they can spread through apps into businesses.

A March report from RAND Corporation "Markets for Cybercrime Tools and Stolen Data" (commissioned by Juniper Networks) correctly predicted that in addition to unpatched vulnerabilities, the human element will continue to increase as the weak point for attacks.

At the end of 2014, 95 percent of IT managers believe that they’re struggling against the biggest threats in the form of mobile devices in the hands of careless employees.

9. Cloud disasters

It’s no surprise that despite the fact that enterprise is rushing to the cloud, enterprise is terrified when it has to think about cloud security and trust in the cloud hit an all time low in 2014.

2014 brought big news of serious cloud security breaches, such as the Xen bug forcing Amazon to reboot its EC2 instances, and Xen making Rackspace do the same this weekend.

Consumer fears were fanned, investors panicked and Apple stock slipped in

the aftermath of the "celebrity nudes iCloud hack". A well-reported exploitation of a known problem with Apple's iCloud security saw the private photos of A-list celebrities published; it was followed with an attack on China's iCloud customers. Apple made cloud security's image worse with a come-lately warning to consumers and after the fact activation of 2FA.

A BT study in September covering 11 countries revealed that more than three-quarters of IT decision makers are "extremely anxious" about security using cloud-based services - yet 79 percent of U.S. enterprise execs (70 percent globally) are adopting cloud storage and web applications within their business.

8. Application security, aka blame the "other services"

Over seven million online service users had their privacy violated and their personal information exposed in just two of 2014's big data thefts - Dropbox and Snapchat - both of which used the blame game to evade critical PR.

A group of malicious hackers got their hands on 6,937,081 Dropbox account credentials and published 1,200 usernames and passwords before asking for Bitcoin to publish even more.

Dropbox issued a statement saying that it had not been hacked, and "These usernames and passwords were unfortunately stolen from other services and used in attempts to log in to Dropbox accounts."

Dubbed "the Snappening" by users of the chat forum 4chan, in October a database containing over 100,000 photos and videos sent across Snapchat networks was leaked online. A third-party Snapchat client app was to blame, which was able to steal images after malicious software installation - exactly what the FCC fined Snapchat for lying about. Snapchat said it was user's fault for the use of 3rd party apps, then tried to not look like absolute jerks by saying they were going to ban 3rd party apps like super really hard with a strongly worded letter from their PR department. In addition to this high-profile attack, the company apologized after 4.6 million Snapchat usernames and matched phone numbers were leaked at the beginning of the year.

7. Facebook scams

Check the news yourself: a new Facebook scam was reported roughly once a week in 2014. Any news headline, scare, or new gadget gets turned into a Facebook scam.

A Facebook study by the security company Bitdefender released in late 2014 unearthed 850,000 Facebook scams running on the social network, dividing into five distinct trends.

Almost half of the scams pretended to allow users to track their profile views, an offer the company said was popular among people wishing to see if former lovers were keeping tabs on them. The problem, researchers concluded, was that due to Facebook's UI (and possibly its design intent), users can't tell what's real, and what's not.

The 2014 cost of these scams per year is estimated at "even higher" than the $12.7 billion global loss to Nigerian scams.

6. The Drupal boogeyman

Drupal nearly won the prize in with a fairly horrible security blunder, when the Drupal team disclosed a really, really bad SQL injection vulnerability in Drupal 7 - and warned that unless you patched within seven hours, you'd be hacked.

Drupal claims a million users on its project site drupal.org, and over 30,000 developers. Many prominent sites, including the whitehouse.gov, use Drupal.

5. Apple's rot

After years of rubbing its secure operating system in everyone's faces, Apple finally rode that reputation into the ground in 2014 with a series of unforgiving security disasters.

February's Goto Fail: A shockingly overlooked SSL encryption issue left iPhone, iPad and Mac computer users open to a man-in-the-middle (MITM) attack and was upsettingly patched in stages. A well-reported exploitation of iCloud security to ruin the (little) privacy of A-list celebrities and a too little, too late warning to consumers (as well as after the fact activation of 2FA) made Apple stocks slide. The attack on China's iCloud customers. Rootpipe. Patching 144 severe vulnerabilities in one update. And much more.

Microsoft had a tough year, too. In the immortal phrasing of the Doge meme - Microsoft: such 0day, many patches.

Microsoft fixed a severe 19-year-old Windows 0day bug found in pretty much everything since Windows 95, issued a bazillion patches, and revealed a vulnerability in most versions of Internet Explorer so bad that government security response teams in the US, the UK, and Sweden urged Windows users to consider Chrome or Firefox as their default browser until Microsoft delivered a fix.

4. China

Hackers from - or working for - China took center stage in 2014 as the role of China's hackers in everything from malware, IP theft and state-sponsored attacks snowballed in headlines up to the end of the year.

In May 2014 the US DoJ indicted five Chinese hackers for committing economic and cyber espionage against several American companies hacking by members of the Chinese military and it represented the first-ever charges against a state actor for this type of hacking. All five are wanted by the FBI but three of them made the FBI's top ten most wanted hackers list (Wen Xinyu, Huang Zhenyu, and Sun Kailiang).

In July, the CrowdStrike team went public saying that several national security-based think tanks were compromised in the defense, finance, legal and government arenas by the Chinese cyberattack group Deep Panda, which the security researchers called "one of the most advanced Chinese nation-state cyber intrusion groups." It was only one of several Chinese hack attacks and groups CrowdStrike found in 2014.

The Chinese government has been accused of backing cyberattacks against Apple's iCloud, initiated in order to steal user credentials. The finger has also been pointed at China for the 2014 hacking of the US Postal System (over 800,000 employees), NOAA, as well as the White House and

US State Department.

3. Shellshock

The Shellshock Unix/Linux Bash security hole emerged in September and immediately was recognized widely as a serious problem: It was estimated to potentially affect around half of the internet's websites. Shellshock serves as a highway for worms and malware to attack Unix, Linux, and Mac servers, as well as affecting mail servers. The bug had been in the Bash shell for 20 years and was widely deployed in a configuration that made it easy to exploit - and it was exploited in the wild within a day of its public debut.

2. Mega Retail Breaches

2014 started on the tail end of Target's massive breach, then continued with Home Depot, Kmart, Michael's, Dairy Queen, Staples, Goodwill, Nieman Marcus, JP Morgan Chase, Verizon, EA Games and many more - heralding the rise of POS malware. To give you an idea of scale, Home Depot said that 53 million email addresses were swiped in its recent data breach where 56 million credit card accounts were also compromised.

The Identity Theft Research Center's 2014 report summary of data breaches paints a disturbing picture of 2014 to date - as of October, there have been 621 known and reported major breaches and 77,890,487 records stolen.

The Banking, Credit and Financial sector saw 24 breaches for 2014, with 1,172,320 records compromised; Business is at a stunning 215 breaches with 64,407,359 records stolen; Medical/Healthcare has also been hit hard this year with 263 successful hacks and 7,464,611 records pilfered.

Research from security analysts at BitSight found that in 2014, the retail industry encountered an increase in infections in every threat indicator it monitors. Malware distribution saw the largest increase, followed by botnet infections. As for the prevalent malware strains, BitSight says it detected an abundance of Maazben, ZeroAccess, Zeus, Viknok, Conficker and Cutwail.

A report conducted by Ponemon Institute on behalf of RSA at the end of 2014 confirmed that in the wake of mega breaches, consumers are reaching a point of "breach fatigue."

1. 2014's threat theme: White-knuckle flaws in TLS/SSL protocols: Goto Fail, Heartbleed, POODLE, WinShock

The Hollywood star of SSL's worst year ever was Heartbleed, the OpenSSL vulnerability that showed up with its own logo and branding - and pissed off companies when the headline-friendly bug was revealed before patches could be delivered for it. Google, AWS, and Rackspace were affected by Heartbleed OpenSSL flaw - but Azure escaped.

Heartbleed is an encryption flaw which can theoretically be used to view apparently secure communication across HTTPS; the data at risk includes everything from passwords and encryption keys to financial details and personal identifiable information - allowing a hacker to dip in, swipe data, and leave no trace of their existence.

The programmer responsible for code leading to Heartbleed said the flaw was accidental.

But before Heartbleed, there was Apple’s February’s Goto Fail, a massive oversight in SSL encryption that left iPhone, iPad and Mac users open to MiTM attacks and - in poor form - was patched in stages.

Late in the year Google released ’nogotofail’ (named in honor of the ’goto fail’ bug that affected Mac and iOS systems in early 2014) a tool which offers a way to confirm that internet-connected devices and applications aren’t vulnerable to transport layer security (TLS) and secure sockets layer (SSL) encryption issues, such as known bugs or misconfigurations.

It was no Heartbleed, but in late fall, Google’s Security Team revealed that the long obsolete, but still all too used, Secure Sockets Layer (SSL) 3.0 cryptographic protocol has a major security flaw. In an example attack called Padding Oracle On Downgraded Legacy Encryption (POODLE), an attacker can steal "secure" HTTP cookies or other bearer tokens such as HTTP Authorization header contents. According to the team’s Bodo Mller: "This vulnerability allows the plaintext of secure connections to be calculated by a network attacker." The OpenSSL Initiative issued a patch.

Microsoft got invited to the SSL-in-Hell party as 2014 came to a close. November’s Patch Tuesday for Microsoft disclosed vulnerability CVE-2014-6321, named by the community "WinShock" - a severe 19-year-old Windows 0day bug found in pretty much everything since Windows 95; Microsoft reports that the SChannel security package is vulnerable on both Windows servers and clients (SChannel is a Security Support Provider (SSP) that implements SSL and TLS authentication protocols.)

2015: The year ahead

Lessons cyberdefense may be able to teach us about managing Ebola
Hacked: The six most common ways non-tech people fall victim
FBI Director: Mobile encryption could lead us to ’very dark place’
Average company now compromised every four days, with no end to the cybercrime wave in sight

It’s easy to see which of 2014’s big bad threats will be confined to 2014, and which will continue if things don’t improve in security education for the ordinary user (especially BYOD attacks), application security, blame games and accountability problems among startups, and the security practices of retailers.

Other things not mentioned on this list are sure to see an increase - such as the tanking state of Android security in 2014 and the end-of-year realizations about Android malware (responsible for 70 percent of all mobile attacks in 2014).

Healthcare security will most certainly be in 2015’s attack spotlight: A late 2014 report from BitSight Technologies analyzed the cybersecurity practices of companies on the S&P 500, with those in the healthcare sector coming in at the bottom of a four-industry pack.

It’s also easy to predict that 2015 will see attacks increase in trends toward larger Internet of Things (IoT) attacks: A late 2014 report shows 95 percent of enterprise are stressed about IoT security.

The end of 2014 saw the FTC shut a scam security company that duped consumers out of $2.5 million by falsely detecting computer viruses and selling bogus antivirus software: With hacking, surveillance and

retail breaches in every other headline, we can expect to see much more of this in 2015.

=~=~=~=